|  |  |
| --- | --- |
|  | THE UNIVERSITY OF BRITISH COLUMBIA (*All UBC Merchants*) |

|  |  |
| --- | --- |
| **Requirement 1: Install and maintain a firewall configuration to protect data** | |
| **Question 1.1.4: *Description of groups, roles, and responsibilities for logical management of network components?*** | |
| **Date of Issue:**  (July 19, 2010) |

**PURPOSE**

To document the procedures to meet PCI compliance requirement (*1.1.4*)

**POLICY**

These procedures relate to university policy 106 (Access to and Security of Administrative Information), and section 5 (PCI-DSS Requirements) of UBC’s Information Security Manual.

This document identifies those groups, IT and otherwise, that impact the logical management of the network components that are within the scope of the PCI Compliance effort. The document will work from the macro-level to the local merchant network component level.

**Granularity:**

1. Internet Service Provider – external to the merchant network

2. UBC IT Core Network and Routers, Domain Name and Time Services

3. Firewall and Internal Networks/VLANs/VRFs

4. Switches and Network Ports at the Physical Room/Patch Panel level

5. Switches, MiniHubs, and POS Equipment at the Room/Location level

**Groups:**

1. **The Network Management Centre (NMC), BCnet monitor and maintain our core networks and related network support services like DNS, NTP, DHCP that may affect merchant network access to the Credit Acquirer Servers. The NMC has a reporting and governance structure within the UBC IT organizational structure. Group A can be viewed to impact mostly levels 1 and 2, with a separate network infrastructure group at UBC IT affecting level 3.**
2. **IT Management at the Department or Faculty level have the access rights – physical and via web management tools, to monitor, modify, report on firewall and logical network configurations like VLANs and VRFs. The roles and responsibilities for change management and logging may be delegates to supporting IT specialists like LAN Coordinators. Access controls (login credentials) are used to restrict access to management interfaces.**
3. **IT Technical Staff, IT Support have physical access to locked communication rooms where network patch panels and building-level network switches and equipment reside. Access control is via keyed physical access and job request systems that log changes to physical plant.**
4. **IT Support at the local level may have access to the physical wiring from the wall ports to switches and cabling that interconnect POS payment devices.**
5. **Non-technical support staff – should not have rights to modify devices and cabling that are within scope of POS PCI Compliance. Do we need to qualify with a supervisory/review note if it’s something like Facilities and Cabling running new network runs?**

**CONTACT INFORMATION**

For document enquiries, please contact (*Kenneth Wong, UBC Bookstore, 2-5817*).

**REVISION HISTORY**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Date** | **Details of Change** | **Changed By** | **Approved By** | **Title** |
| (*July 19, 2010*) | (*1.0*) | (*Ken Wong, Bookstore*) | (Ken Wong, initial document) | (*Systems Manager, Bookstore*) |